

BRIAN J. STRETCH (CABN 163973)
United States Attorney

DAVID R. CALLAWAY (CABN 121782)
Chief, Criminal Division

S. WAQAR HASIB (CABN 234818)
JEFFREY SHIH (CABN 296945)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
waqar.hasib@usdoj.gov; 415-436-7261
jeffrey.shih@usdoj.gov; 415-436-7168

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,) CASE NO. 3:15-CR-582-WHO
)
Plaintiff,) PROTECTIVE ORDER PERTAINING TO
) CLASSIFIED INFORMATION PURSUANT TO
v.) CLASSIFIED INFORMATION PROCEDURES
) ACT
ADAM SHAFI,)
)
Defendant.)
)

This matter comes before the Court upon the United States' Motion for a Protective Order Pursuant to the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3, to protect against the unauthorized use, disclosure, or dissemination of classified information and documents that will be made available to and reviewed by, or are otherwise in the possession of, defense counsel in this case.

Pursuant to the authority granted under Sections 3 and 9 of CIPA, the Security Procedures Established Pursuant to Pub.L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (the "Security Procedures Established by the Chief Justice"),

1 Federal Rules of Criminal Procedure 16(d) and 57, and the general supervisory authority of the Court,
 2 and in order to protect the national security, the following IS HEREBY ORDERED:

3 1. The Court finds that this case will involve classified national security information. The
 4 storage, handling, and control of this information require special security precautions mandated by
 5 statute, executive order, and regulation, and access to this information requires the appropriate security
 6 clearance and a “need-to-know” determination pursuant to Executive Order 13526, as amended.

7 2. The purpose of this CIPA Protective Order (“Order”) is to establish the procedures that
 8 must be followed by all counsel of record and any other person who receives access to, or otherwise is in
 9 possession of, classified information in connection with this case.

10 3. These procedures shall apply to all pre-trial, trial, post-trial, and appellate matters in this
 11 case, and may be modified by further order of the Court pursuant to Sections 3 and 9 of CIPA, the
 12 Security Procedures Established by the Chief Justice, Federal Rules of Criminal Procedure 16(d) and 57,
 13 and the Court’s inherent supervisory authority to ensure a fair and expeditious trial.

14 **DEFINITIONS**

15 4. The following definitions shall apply to this Order:

16 A. The terms “classified information,” “classified document,” or “classified
 17 material” shall include:

18 (i) any information, document, or material that has been classified by any
 19 Executive Branch agency in the interest of national security or pursuant to Executive
 20 Order 13526, as amended, or its predecessors, as “CONFIDENTIAL,” “SECRET,” or
 21 “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED
 22 INFORMATION”;

23 (ii) any information, document, or material that includes “foreign government
 24 information,” as that term is defined in Executive Order 13526, as amended, or its
 25 predecessors, regardless of place of origin;

1 (iii) any information, document, or material, even if now or formerly in the
2 possession of a private party, that has been derived from classified information; and

3 (iv) any information, document, or material of which defense counsel has been
4 notified, knows, or reasonably should know contains classified information, such as
5 information relating to national security or intelligence matters.

6 B. The terms “information,” “document,” and “material” shall include, but are not
7 limited to, all written, printed, or verbally-conveyed matter of any kind, formal or informal,
8 including originals, conforming copies and non-conforming copies (whether different from the
9 original by reason of notation made on such copies or otherwise). The terms “information,”
10 “document,” and “material” shall further include, but are not limited to, the following regardless
11 of form or characteristics:

12 (i) Papers, correspondence, memoranda, notes, letters, reports, summaries,
13 photographs, maps, charts and graphs, interoffice and intra-office communications,
14 notations of any sort concerning conversations, meetings or other communications,
15 bulletins, teletypes, telegrams and telefacsimiles, invoices, worksheets and drafts,
16 alterations, modifications, changes, and amendments of any kind to the foregoing;

17 (ii) Graphic records or representations of any kind, including but not limited
18 to photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of
19 any kind, and motion pictures;

20 (iii) Electronic, mechanical or electric records of any kind, including but not
21 limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing
22 or other computer tapes or disks, and all manner of electronic data processing storage;
23 and

24 (iv) Any form of document reflecting information acquired orally or verbally.
25

1 C. The term “access to classified information” means having access to, reviewing,
 2 reading, listening to, learning, or otherwise coming to know in any manner any classified
 3 information.

4 D. The term “Secure Area” shall mean a physical facility approved by the Classified
 5 Information Security Officer for the storage, handling, and control of classified information.

6 **CLASSIFIED INFORMATION SECURITY PROCEDURES**

7 5. All classified information, and the information contained therein, shall remain classified
 8 unless the information bears a clear indication that they have been “declassified” by the agency or
 9 department that originated the information contained therein (hereinafter the “Originating Agency”).
 10 Information that is classified that also appears in the public domain is not thereby automatically
 11 declassified unless it appears in the public domain as the result of the Originating Agency declassifying
 12 the information.

13 6. *Classified Information Security Officer.* In accordance with the provisions of CIPA and
 14 the Security Procedures Established by the Chief Justice, the Court designates Winfield S. “Scooter”
 15 Slade as Classified Information Security Officer (“CISO”) for this case, and Debra M. Guerrero-
 16 Randall, Daniel O. Hartenstine, Joan B. Kennedy, Michael P. Macisso, Maura L. Peterson, Carli V.
 17 Rodriguez-Feo, and Harry J. Rucker as Alternate CISOs, for the purpose of providing security
 18 arrangements necessary to protect from unauthorized disclosure any classified information to be made
 19 available in connection with this case. Defense counsel shall seek guidance from the CISO with regard
 20 to appropriate storage, handling, transmittal, and use of classified information.

21 7. *Government Counsel.* The Court has been advised by the CISO that the Government
 22 attorneys working on this case, Assistant United States Attorneys S. Waqar Hasib and Jeffrey L. Shih,
 23 their supervisors, and certain other Department of Justice employees (collectively, “Government
 24 Counsel”), have the requisite security clearances allowing them to have access to the classified
 25 information that relates to this case.

1 8. *Clearance Prerequisites for Defense Access to Classified Information.* The Court finds
 2 that, in order to protect the classified information involved in this case, only the appropriately-cleared
 3 defense counsel, and employees or contractors (e.g., investigators, paralegals, experts, or translators) of
 4 defense counsel (the “Defense”) may have access to the classified information in this case.

5 A. No defense counsel, or employees or contractors of defense counsel, may have
 6 such access until first obtaining the appropriate clearance. Each person on the Defense who
 7 seeks such clearance must complete or obtain all three of the following:

8 (i) *Need-to-Know.* The defense counsel, or employee or contractor of defense
 9 counsel, must receive permission of the Court, either through this Order (*i.e.*, for those
 10 named or listed in Paragraph 8.B below) or by a separate Court order upon showing of a
 11 “need-to-know” the classified information in this case.

12 (ii) *Security Clearance.* The defense counsel, or employee or contractor of
 13 defense counsel, must receive the necessary security clearance at the level of the
 14 classified information involved in this case, through or confirmed by the CISO. The
 15 forms, releases, and fingerprints shall be completed and submitted to the CISO forthwith
 16 by all defense counsel and employees or contractors of defense counsel who are not
 17 otherwise already cleared and whose assistance the defense reasonably requires to have
 18 access to the classified information in this case. The CISO will take all reasonable steps
 19 necessary to process security clearance applications in accordance with applicable laws
 20 and regulations.

21 (iii) *Memorandum of Understanding (“MOU”).* The defense counsel, or
 22 employee or contractor of defense counsel, must sign the MOU in the form attached
 23 hereto, agreeing to comply with the terms of this Order, file the original of the executed
 24 MOU with the Court and the CISO, and serve a copy on Government Counsel. The
 25 substitution, departure, or removal for any reason from this case of any defense counsel,

1 or any employee or contractor of defense counsel, shall not release that person from the
2 provisions of this Order or the Memorandum of Understanding executed in connection
3 with this Order.

4 B. Through this Order, subject to the other prerequisites of Paragraph 8.A above, the
5 Court finds that the following defense counsel have a “need-to-know” the classified information
6 in this case as required by the Government’s discovery obligations: Assistant Federal Public
7 Defender Galia Amram.

8 9. *Secure Area for the Defense.* The CISO shall arrange for an appropriately approved
9 Secure Area for use by the Defense. The CISO shall establish procedures to assure that the Secure Area
10 is accessible to the Defense during normal business hours, and at other times upon reasonable request as
11 approved by the CISO in consultation with the U.S. Marshals Service. The Secure Area shall contain a
12 separate working area for the Defense and will be outfitted with any secure office equipment requested
13 by the Defense that is reasonable and necessary to the preparation of the defense in this case. The CISO,
14 in consultation with the Defense, shall establish procedures to assure that the Secure Area may be
15 maintained and operated in the most efficient manner consistent with the protection of classified
16 information. No classified information, document, or material may be removed from the Secure Area
17 unless so authorized by the CISO. The Secure Area shall not be accessible to Government Counsel, and
18 the CISO shall not reveal to Government Counsel the content of any conversations that the CISO may
19 hear among the Defense, nor reveal the nature of the information, documents, or material being
20 reviewed or the work being generated by the Defense. The presence of the CISO shall not operate to
21 waive, limit, or otherwise render inapplicable the attorney-client or work product privilege.

22 10. *Access to Classified Information by the Defense.* The Defense shall have access to
23 classified information only as follows:

24 A. All classified information provided to the Defense by the Government is to be
25 used solely by the Defense and solely for the purpose of preparing the defense. The Defense

1 may not use, disclose, or cause to be disclosed any information known or reasonably believed to
2 be classified information except as otherwise provided in this Order.

3 B. All classified information produced by the Government to the Defense, in
4 discovery or otherwise, and all classified information possessed, created, or maintained by the
5 Defense, including notes and any work product, shall be stored, maintained and used only in the
6 Secure Area established by the CISO.

7 C. The Defense shall have free access to the classified information made available to
8 them in the Secure Area, and shall be allowed to take notes and prepare documents with respect
9 to those materials.

10 D. The Defense (and representatives of the Defense, such as counsel, investigators,
11 paralegals, translators, experts, and witnesses) shall not copy or reproduce any classified
12 information in any form except with the approval of the CISO or in accordance with the
13 procedures established by the CISO for the operation of the Secure Area.

14 E. All documents prepared by the Defense (including, without limitation, motions,
15 memoranda, or other documents intended for filing with the Court) that do or may contain
16 classified information must be prepared (e.g., transcribed, recorded, typed, duplicated, copied) in
17 the Secure Area on equipment approved by the CISO, only by persons who have completed and
18 obtained the clearance prerequisites defined in Paragraph 8 above in order to access classified
19 information, and in accordance with the procedures approved by the CISO. All such documents
20 and any associated materials (such as notes, drafts, copies, electronic media, exhibits, etc.)
21 containing classified information shall be maintained in the Secure Area, unless and until the
22 CISO determines that those documents or associated materials are unclassified in their entirety.
23 None of these materials shall be disclosed to Government Counsel.

24 F. The Defense shall discuss classified information only within the Secure Area or in
25 another area authorized by the CISO. The Defense shall not discuss or attempt to discuss

1 classified information over any standard commercial telephone instrument, office
2 intercommunication system, or any other method of communication (e.g., the Internet) not
3 specifically authorized by the CISO.

4 G. The Defense shall not disclose, without prior approval of the Court, any classified
5 information to or in the presence of any person not authorized pursuant to this Order, including
6 the defendant and defense witnesses, except the Court, court personnel, and Government
7 Counsel who have been identified by the CISO as having the appropriate clearances and the
8 need-to-know that information. If preparation of the defense requires that classified information
9 be disclosed to persons not named in this Order, Government Counsel shall be given prior notice
10 by the Defense and an opportunity by the Court to be heard in response. Any person approved
11 by the Court for disclosure under this paragraph shall be required to complete and to obtain the
12 clearance prerequisites defined in Paragraph 8 above in order to access classified information.

13 11. *Procedures for Use or Disclosure of Classified Information by the Defense.* Procedures
14 for the use or disclosure of classified information by the Defense in any manner in connection with any
15 pretrial or trial proceeding shall be those provided in CIPA (including but not limited to CIPA Sections
16 5, 6, and 8) and this Protective Order. Such procedures include the following:

17 A. The Defense shall not use, disclose, or cause to be disclosed any information that
18 the Defense knows or has reason to believe contains classified information in whole or in part
19 unless and until: (i) the Defense files the notice required by and complies with the requirements
20 of CIPA Section 5; and (ii) after such notice, the Government is afforded a reasonable
21 opportunity to seek a determination pursuant to the procedures of CIPA Section 6, and the time
22 to appeal such a determination has expired or the appeal is decided under CIPA Section 7. Use
23 and disclosure of classified information includes any attempt (e.g., eliciting testimony) by the
24 Defense to have such information confirmed or denied at any public proceeding in this case.
25

1 B. In the event that classified information enters the public domain, the Defense shall
2 not confirm or deny classified information that appears in the public domain unless the Defense
3 first complies with the requirements of CIPA, including the procedures in Paragraph 11.A above.

4 12. *Filings with the Court by the Defense.* Any motion, memorandum, or other document
5 filed by the Defense that the Defense knows, or has reason to believe, contains classified information in
6 whole or in part, or any document the proper classification of which the Defense is unsure, shall be filed
7 as follows:

8 A. The Defense shall complete each of the following: (i) The Defense shall mark the
9 document, "Filed With The Classified Information Security Officer, In Camera, Under Seal,"
10 and shall include an introductory statement that it is being filed under seal pursuant to this Order,
11 but need not be accompanied by a separate motion to seal. (ii) The Defense shall file the
12 document under seal with the Court by physically submitting the document to the CISO, or the
13 CISO's designee. The date and time of the physical submission to the CISO, or the CISO's
14 designee, shall be considered as the date and time of the court filing. (iii) At the time of making
15 a physical submission to the CISO, or the CISO's designee, the Defense shall file on the public
16 record in the CM/ECF system a notice of filing. The notice should contain only the case caption,
17 an unclassified title of the filing, and notice that the submission was made to the CISO or the
18 CISO's designee.

19 B. The CISO shall promptly examine the document and, in consultation with
20 representatives of the appropriate Government agencies, determine whether the document
21 contains classified information. If the CISO determines that the document contains classified
22 information, he or she shall ensure that the classified portions of the document, and only those
23 portions, are marked with the appropriate classification marking and that the document remains
24 under seal. If the CISO determines that the document contains no classified information, the
25

1 document filed by the Defense shall immediately be unsealed by the CISO and placed in the
2 public record.

3 C. The CISO shall make arrangements for the prompt delivery under seal to the
4 Court, and to Government Counsel unless the filing is ex parte, any document to be filed by the
5 Defense that contains classified information.

6 13. *Filings with the Court by Government Counsel.* Any motion, memorandum, or other
7 document filed by Government Counsel that contains classified information shall be filed as follows:

8 A. Government Counsel shall complete each of the following items specified in
9 Paragraph 12.A above.

10 B. The CISO shall make arrangements for the prompt delivery under seal to the
11 Court, and to the Defense unless the filing is ex parte, any document to be filed by Government
12 Counsel that contains classified information.

13 14. *Record and Maintenance of Classified Filings.* The CISO shall maintain a separate
14 sealed record for those filings containing classified information and retain such record for purposes of
15 later proceedings or appeal.

16 15. *Violations of this Order.* Unauthorized use or disclosure of classified information may
17 constitute violations of United States criminal laws. In addition, violation of the terms of this Order
18 shall be immediately brought to the attention of the Court, and may result in a charge of contempt of
19 Court and possible referral for criminal prosecution. Any breach of this Order may result in the
20 termination of a person's access to classified information. Persons subject to this Order are advised that
21 direct or indirect unauthorized use, disclosure, retention or negligent handling of classified information
22 could cause serious damage, and in some cases exceptionally grave damage, to the national security of
23 the United States, or may be used to the advantage of a foreign nation against the interests of the United
24 States. This Order is to ensure that those authorized to receive classified information will never divulge
25 the classified information disclosed to them to anyone who is not authorized to receive it, and will never

1 otherwise use the classified information without prior written authorization from the Originating Agency
2 and in conformity with this Order.

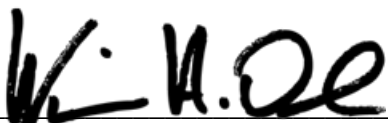
3 16. All classified information to which the Defense has access in this case is now and will
4 remain the property of the Government. Upon demand of the CISO, the Defense (and representatives of
5 the Defense, such as counsel, investigators, paralegals, translators, experts, and witnesses) and anyone
6 else who receives classified information pursuant to this Order shall return all such classified
7 information in their possession obtained through discovery from the Government in this case or for
8 which they are responsible because of access to classified information. The notes, documents, and other
9 work product prepared by the Defense that do or may contain classified information shall remain at all
10 times in the custody of the CISO for the duration of this case. At the conclusion of all proceedings,
11 including any final appeals, all such notes, documents, and other work product are to be destroyed by the
12 CISO, and in the presence of defense counsel if so requested.

13 17. Nothing in this Order shall preclude the Government from seeking a further protective
14 order pursuant to CIPA and/or Federal Rule of Criminal Procedure 16(d) as to particular items of
15 discovery material.

16 18. A copy of this Order shall be issued forthwith to defense counsel, who shall be
17 responsible for advising the defendant and representatives of the Defense of this Order.

18
19 IT IS SO ORDERED.

20
21 Dated: June 13, 2016

22 
HONORABLE WILLIAM H. ORRICK
UNITED STATES DISTRICT JUDGE